ALGEBRAS, GROUPS AND GEOMETRIES 40 11 – 21 (2024)
DOI 10.29083/AGG.40.01.2024/SC11

AN APPLICATION OF SMITH NORMAL FORM

Haohao Wang
Department of Mathematics
Southeast Missouri State University
Cape Girardeau, MO 63701
hwang@semo.edu

Received February 13, 2024

Abstract

Modules are a generalization of the vector spaces of linear algebra over a ring instead of over a field of scalars. Some of the results in linear algebra are extremely useful in studying modules. In this paper, we highlight the use of Smith normal form in studying finitely generated modules over a univariate polynomial ring. As an application, we take advantage of Smith normal form to understand the structure of certain syzygy modules.

Keywords: Module; Basis; Smith Normal Form; PID.

1 Introduction

Linear algebra deals with vector spaces and linear transformations over a field such as real or complex numbers. Linear algebra is very well understood, serves as a fundamental tool for mathematical economics, data science, machine learning, and has many applications, from mathematical physics to modern algebra and coding theory.

Modules are a generalization of the vector spaces of linear algebra over a ring instead of over a field of scalars. A fundamental fact of linear algebra over a field is a finitely generated vector space has a basis – the minimal generating (spanning) set of a vector space are linearly independent and therefore form a basis. However, modules are more complicated than vector spaces; for instance, not all modules have a basis. Only a special family of modules called *free modules* have a basis. It remains an interesting and an active research area to find the minimal generating set, or an upper bound for the minimal generating set for different kinds of modules under various of conditions [2], [3], [4], and [6].

In linear algebra, matrix factorization is a mathematical technique used to decompose a matrix into the product of multiple matrices. There are various ways to decompose a matrix depending on the context in which that matrix is used. For instance, in computer science and machine learning, singular value decomposition is one of the most important computational method. Whereas, representing a matrix in the Smith normal form has many computational applications in number theory, group theory, and homological algebra.

In this short paper, we focus on the Smith normal form, and its applications in modules over univariate polynomial rings $\mathbb{K}[x]$ with $\mathbb{K}$ an algebraically closed field of characteristic zero. Our goal is to find a minimal set of generators for certain syzygy modules using Smith normal form.

Recall that given a generating set $\{f_1, \ldots, f_m\}$ of an ideal (or a module) over a ring R, a relation or the first *syzygy* between the generators is an m-tuple $(a_1, \ldots, a_m) \in R^m$ such that

$$a_1 f_1 + a_2 f_2 + \cdots a_m f_m \equiv 0.$$

The set of syzygies form a *syzygy module,* denoted by $S = \mathrm{Syz}(f_1, \ldots, f_m)$. A *Koszul syzygy* is one of the form

$$(f_j)f_i + (-f_i)f_j = 0, \text{ for } i \neq j.$$

The Koszul syzygies generate a submodule of the syzygy module S.

Our attention is centered on the submodule K that are generated by the "Koszul-like" forms over a univariate polynomial ring $\mathbb{K}[x]$:

$$\left[0, \cdots, 0, -\frac{f_j}{\gcd(f_i, f_j)}, 0, \cdots, 0, \frac{f_i}{\gcd(f_i, f_j)}, 0, \cdots, 0\right]^T, \ 1 \leq i < j \leq m.$$

We seek the answers to the question that how the minimal sets of generators for K and S are related.

This paper is structured as the following. We begin in Section 2 with a brief review of results concerning the Smith normal form over Principal Ideal Domains (PIDs), and the Hilbert–Burch Theorem. We then study the minimal set of generators for the submodule K of a syzygy module S in Section 3. The main results of this paper are Theorems 3.1 and 3.2, where we provide an explicit equation to describe a relationship between a basis for K and a basis for S. We flush out our theorems by a simple and illustrative example.

2 A Brief Review

The Smith Normal Form (SNF) is a canonical form to which a matrix can be transformed using elementary row and column operations. It is particularly useful when dealing with matrices whose entries come from a ring with special properties, such as PIDs. Theorem 2.1 is a well-known results concerning SNF over PID.

Theorem 2.1. *(Smith Normal Form over PID [1, Theorem 3.1]) Let R be a PID and let $A \in M_{m,n}(R)$. Then there is a $U \in GL(m, R)$ and a $V \in GL(n, R)$ such that*

$$UAV = \begin{bmatrix} D_r & 0 \\ 0 & 0 \end{bmatrix},$$

where $r = \text{rank}(A)$, *and* D *is a diagonal matrix with diagonal entries* $s_1, s_2, \ldots, s_r$ *with* $s_i \neq 0$ *for* $i = 1, \ldots, r$, *and* $s_i \mid s_{i+1}$ *for* $i = 1, \ldots, r-1$. *Additionally,* s_i*'s are unique up to multiplication by a unit and are called the elementary divisors, invariants, or invariant factors, which can be computed (up to multiplication by a unit) as* $s_i = \frac{d_i(A)}{d_{i-1}(A)}$, *where* $d_i(A)$ *is called* i*-th determinant divisor that equals the greatest common divisor of the determinants of all* $i \times i$ *minors of the matrix* A *and* $d_0(A) := 1$. *Furthermore, if* R *is a Euclidean domain, the matrices* U, V *can be taken to be a product of elementary matrices.*

In the context of modules (generalizations of vector spaces) over a PID, the SNF reveals important information about the structure of the module and its relationship to other modules. Throughout this paper, we should use Theorem 2.1 to investigate the minimal set of generators for modules. To our advantage, we refer SNF as the matrix factorization that decomposes A into the product of invertible matrices with a diagonal matrix, and write $A = U \begin{bmatrix} D_r & 0 \\ 0 & 0 \end{bmatrix} V$ for some invertible matrices U, V.

For the convenience of our readers, we also cite a part of the Hilbert–Burch Theorem below. The complete statement of the Hilbert–Burch Theorem is beyond the scope of this paper, we only cite the portion of the theorem that concerns the first syzygy module $\text{Syz}(f_1, \ldots, f_m)$ over $\mathbb{K}[x]$.

Theorem 2.2. *(Hilbert–Burch Theorem [5]) If* M *is a module minimal generated by* m *elements over a polynomial ring* $\mathbb{K}[x]$ *over a field* $\mathbb{K}$, *then the first syzygy module of* M *is always a free module of rank* $m - 1$.

We want to emphasize that this result states that the first syzygy module $\text{Syz}(f_1, \ldots, f_m)$ has a basis consisting of $m - 1$ linearly independent generators over univariate polynomial rings; however, it is not true in general for multivariate polynomial rings.

3 Main Results

Theorem 3.1. *Let* $\{p_1, \ldots, p_{m-1}\}$ *be a basis for the syzygy module* $S = \text{Syz}(f_1, \ldots, f_m)$ *where* $f_1, \ldots, f_m \in R = \mathbb{K}[x]$. *Let* K *be the submodule*

generated by the syzygies of the form

$$\left[0,\cdots,0,-\frac{f_j}{\gcd(f_i,f_j)},0,\cdots,0,\frac{f_i}{\gcd(f_i,f_j)},0,\cdots,0\right]^T,\ 1\le i<j\le m.$$

Then

1. *K is minimally generated by $m-1$ syzygies of such form, that is,* $\operatorname{rank}(K)=m-1$.
2. *There exist at most $m-1$ distinct $C_1,\ldots,C_{m-1}\in R$ where C_i is the smallest degree element in R such that $C_ip_i\in K$.*
3. *The colon ideal $\langle K:S\rangle=\{r\in R\mid rS\subseteq K\}$ is the principle ideal generated by $C=\operatorname{LCM}(C_1,\ldots,C_{m-1})$, the least common multiple of $C_1,\ldots,C_{m-1}$, that is, $\langle K:S\rangle=\langle\operatorname{LCM}(C_1,\ldots,C_{m-1})\rangle=\langle C\rangle$,*
4. *$S/K\cong R/\langle t_1\rangle\times R/\langle t_2\rangle\times\cdots\times R/\langle t_{m-1}\rangle$, where $t_1,\ldots,t_{m-1}$ are the elementary divisors of T for some T such that $K=ST$.*

Proof. Let K be a syzygy submodule generated by the columns of the matrix

$$\begin{bmatrix}
\frac{-f_m}{\gcd(f_1,f_m)} & \frac{-f_{m-1}}{\gcd(f_1,f_{m-1})} & \cdots & 0 & 0 & \cdots & 0\\
0 & 0 & \cdots & \frac{-f_m}{\gcd(f_2,f_m)} & \frac{-f_{m-1}}{\gcd(f_2,f_{m-1})} & \cdots & 0\\
0 & 0 & \cdots & 0 & 0 & \cdots & 0\\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\
0 & \frac{f_1}{\gcd(f_1,f_{m-1})} & \cdots & 0 & \frac{f_2}{\gcd(f_2,f_{m-1})} & \cdots & \frac{-f_m}{\gcd(f_m,f_{m-1})}\\
\frac{f_1}{\gcd(f_1,f_m)} & 0 & \cdots & \frac{f_2}{\gcd(f_2,f_m)} & 0 & \cdots & \frac{f_{m-1}}{\gcd(f_m,f_{m-1})}
\end{bmatrix}.$$

This matrix is of size $m\times l$ where $l=\binom{m}{2}$. To simplify the the matrix expression, let K_i for $i=1,\ldots,l$ be the i-th column of the above matrix.

Proof of item 1. It is easy to observe that the $(m-1)\times(m-1)$ submatrix formed by the first $m-1$ columns and the last $m-1$ rows has a non-zero determinant. Hence the rank of this matrix is at least $m-1$, i.e., $\operatorname{rank}(K)\ge m-1$. On the other hand, since K is a submodule of S, $\operatorname{rank}(K)\le\operatorname{rank}(S)$, and $\operatorname{rank}(S)=m-1$ by Theorem 2.2. Thus, $\operatorname{rank}(K)=m-1$.

Proof of item 2. Without loss of generality, we may select $m-1$ columns of the matrix that generate the submodule K, and name these generators $K_1, K_2, \ldots, K_{m-1}$. Let $a = [a_1, \ldots, a_m]^T \in S$. Since the matrix $[K_1, K_2, \ldots, K_{m-1}] \in M_{m,m-1}(R)$ is of rank $m-1$, the matrix equation $[K_1, \ldots, K_{m-1}]X = a$ has a unique solution over the function field of R, i.e.

$$X = \left[b_1/c_1, b_2/c_2, \cdots, b_{m-1}/c_{m-1}\right]^T \in (\mathbb{K}(x))^{m-1}, \text{ with } \gcd(b_i, c_i) = 1.$$

Let $c = \mathrm{LCM}(c_1, c_2, \ldots, c_{m-1}) \in \mathbb{K}[x]$, set $c_i' = \frac{c}{c_i}$ for $i = 1, \ldots, m-1$. Then $c_i' \in \mathbb{K}[x]$, $cX = [c_1'b_1, c_2'b_2, \ldots, c_{m-1}'b_{m-1}]^T \in (\mathbb{K}[x])^{m-1}$, and

$$\begin{aligned} ca &= c([K_1, \ldots, K_{m-1}]X) = [K_1, \ldots, K_{m-1}](cX) \\ &= \left[K_1, K_2, \ldots, K_{m-1}\right] \begin{bmatrix} c_1'b_1 \\ c_2'b_2 \\ \vdots \\ c_{m-1}'b_{m-1} \end{bmatrix} = \sum_{i=1}^{m-1} (c_i'b_i)K_i \in K. \end{aligned}$$

Note since $c = \mathrm{LCM}(c_1, c_2, \ldots, c_{m-1})$, up to a constant multiple, c is the smallest degree element in R such that $ca \in K$. That is, for any factor β of c that is not a constant multiple of c, $\beta a \notin K$.

Since $\{p_1, \ldots, p_{m-1}\}$ is a basis for S, by the above argument, there exists at most $m-1$ distinct $C_1, C_2, \ldots, C_{m-1} \in R$ where C_i is the smallest degree element in R such that $C_i p_i \in K$ for each i.

Proof of item 3. Let $C = \mathrm{LCM}\,(C_1, \ldots, C_{m-1})$, then $C_i p_i \in K$ for each i yields that $Cp_i \in K$. Thus, for any $a \in S$, $a = \beta_1 p_1 + \cdots \beta_{m-1} p_{m-1}$ for some $\beta_1, \ldots, \beta_{m-1} \in R$, and

$$Ca = C(\beta_1 p_1 + \cdots + \beta_{m-1} p_{m-1}) = \beta_1(Cp_1) + \cdots + \beta_{m-1}(Cp_{m-1}) \in K.$$

Therefore, we have $\langle K : S \rangle = \langle C \rangle = \langle \mathrm{LCM}\,(C_1, \ldots, C_{m-1}) \rangle$.

Proof of item 4. Since K is a submodule of S, so the generators $K_1, \ldots, K_{m-1}$ of K can be expressed as $K_i = \sum_{j=1}^{m-1} \beta_{ji} p_j$ for some $\beta_{ji} \in R$. Thus, $K = ST$ where $T = [\beta_{ji}]_{i,j=1,\ldots,m-1} \in M_{m-1,m-1}$.

By Theorem 2.1, $T = UDV$ for some invertible $U, V \in M_{m-1,m-1}$ and

$$D = \begin{bmatrix} t_1 & 0 & \cdots & 0 \\ 0 & t_2 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & t_{m-1} \end{bmatrix} \text{ where } t_i \text{ are the elementary divisors of } T.$$

$$K = ST = SUDV \quad \Longleftrightarrow \quad KV^{-1} = (SU)D.$$

Since the columns of $KV^{-1} = [K'_1, \ldots, K'_{m-1}]$ is another basis for K; and similarly, columns of $SU = [p'_1, \ldots, p'_{m-1}]$ is another basis for S. Thus, we have the equality of the matrices

$$[K'_1, \ldots, K'_{m-1}] = KV^{-1} = (SU)D = [t_1 p'_1, \ldots, t_{m-1} p'_{m-1}].$$

Thus consider the following map

$$\phi: \begin{array}{ccc} R \times R \times \cdots \times R & \rightarrow & (SU)/(KV^{-1}) \cong S/K \\ (r_1, r_2, \ldots, r_{m-1}) & \rightarrow & r_1 p'_1 + \cdots + r_{m-1} p'_{m-1}. \end{array}$$

We see that

$$\begin{aligned} \ker(\phi) &= \{(r_1, \ldots, r_{m-1}) \in R^{m-1} \mid \sum_{i=1}^{m-1} r_i p'_i \in KV^{-1}\} \\ &= \langle t_1 \rangle \times \langle t_2 \rangle \times \cdots \langle t_{m-1} \rangle. \end{aligned}$$

Therefore,

$$S/K \cong (SU)/(KV^{-1}) \cong R/\langle t_1 \rangle \times R/\langle t_2 \rangle \times \cdots \times R/\langle t_{m-1} \rangle.$$

□

We want to emphasize that Theorem 3.1 is true under the condition that the polynomial ring is univariate, and not true in general for multivariate polynomial rings.

Next, we will continue with the notations used in Theorem 3.1, and show that SNF stated in Theorem 2.1 can be used to identify a some special properties of syzygy modules.

Theorem 3.2. *Let $S = [p_1, \ldots, p_{m-1}] \in M_{m,m-1}$ whose columns are the minimal set of generators of the syzygy module S of $f_1, \ldots, f_m$; and $K = [K_1, \ldots, K_{m-1}]$ whose columns are the minimal set of generators for the "Koszul-like" syzygy submodule K over the univariable polynomial ring $R = \mathbb{K}[x]$ obtained in Theorem 3.1. Let $K = UDV$ be the SNF for K. Then the last row U_m of the matrix U^{-1} is a constant multiples of $f_1, \ldots, f_m$.*

Proof. First, we express part 2 of Theorem 3.1 in term the following matrix equation:

$$[C_1 p_1, \ldots, C_{m-1} p_{m-1}] = [p_1, \ldots, p_{m-1}] \begin{bmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & C_{m-1} \end{bmatrix}$$

$$= KQ \text{ for some } Q \in M_{m-1,m-1}$$

$$= UDVQ = U \begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & d_{m-1} \\ 0 & 0 & \cdots & 0 \end{bmatrix} VQ$$

where U, V are invertible $U \in M_{m,m}$, $V \in M_{m-1,m-1}$, $D \in M_{m,m-1}$.

Multiplying both sides by U^{-1} yields

$$U^{-1}[C_1 p_1, C_2 p_2, \ldots, C_{m-1} p_{m-1}] = \begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & d_{m-1} \\ 0 & 0 & \cdots & 0 \end{bmatrix} VQ,$$

and the last row of this matrix equation gives

$$U_m[C_1 p_1, C_2 p_2, \ldots, C_{m-1} p_{m-1}] = [0, 0, \ldots, 0]$$
$$\Longrightarrow \quad U_m(C_i p_i) = C_i(U_m p_i) = 0 \quad \Longrightarrow \quad U_m p_i = 0, \ \forall i = 1, \ldots, m-1$$
$$\Longrightarrow \quad U_m \text{ is orthogonal to } p_i, \ \forall i = 1, \ldots, m-1.$$

Since $\{p_1, p_2, \ldots, p_{m-1}\}$ is a minimal set of generators for the syzygy module of $f_1, \ldots, f_m$, we must have $[f_1, \ldots, f_m]$ is orthogonal to each p_i for $i = 1, \ldots, m-1$. Since $S = [p_1, \ldots, p_{m-1}]$ and $\text{rank}(S) = m-1$, the rank of null space of S is one. Hence $U_m = \beta[f_1, \ldots, f_m]$ for some $\beta \in R = \mathbb{K}[x]$. Now, the fact that U is invertible over R implies that $\det(U) \in \mathbb{K}$. Therefore, $\beta \in \mathbb{K}$, otherwise $\det(U)$ would have a non-constant polynomial as a factor, contradicting to the fact that U is invertible.

Thus, we conclude that the last row U_m of the matrix U^{-1} is a constant multiples of $f_1, \ldots, f_m$.

□

We shall use the following example to illustrate the the results in Theorem 3.1 and Theorem 3.2.

Example 3.3. *Consider* $[f_1, f_2, f_3] = [1, x^2-1, x^3+1]$. *One can compute a minimal set of generators for the syzygy module* $\text{Syz}(f_1, f_2, f_3)$ *is formed by the columns of the matrix* $S = [p_1, p_2] = \begin{bmatrix} x^2-1 & x^3+1 \\ -1 & 0 \\ 0 & -1 \end{bmatrix}$.

The submodule K *is generated by the syzygies in the columns of the matrix*

$$[K_1, K_2, K_3] = \begin{bmatrix} x^2-1 & x^3+1 & 0 \\ -1 & 0 & x^2-x+1 \\ 0 & -1 & -(x-1) \end{bmatrix}.$$

Since $K_3 = -(x^2-x+1)K_1 + (x-1)K_2$, *the submodule* K *is minimally generated by* K_1, K_2. *We will write* $K = [K_1, K_2]$. *We note that* $K_1 = p_1$, *and* $-xK_1 + K_2 = p_2$, *that is*

$$\begin{aligned} [K_1, K_2]\begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} x^2-1 & x^3+1 \\ -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} x^2-1 & x+1 \\ -1 & x \\ 0 & -1 \end{bmatrix} \\ &= [p_1, p_2]. \end{aligned}$$

Following the notation of Theorem 3.1, $C_1 = C_2 = 1$, *and therefore,*

$$\langle K : S \rangle = \langle \text{LCM}(C_1, C_2) \rangle = \langle 1 \rangle. \quad \Longrightarrow \quad S \cong K.$$

This can also be verified as the following. Since $\begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$,

$$\begin{aligned} [K_1, K_2] &= \begin{bmatrix} x^2-1 & x^3+1 \\ -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} x^2-1 & x+1 \\ -1 & x \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix}^{-1} \\ &= [p_1, p_2]T = ST \ \textit{where}\ T = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

In terms of Theorem 3.1 (4.), the elementary divisors of T *are:* $t_1 = t_2 = 1$. *Hence* $S/K \cong R/\langle 1\rangle \times R/\langle 1\rangle \cong 0$, *that is,* $S \cong K$.

Now, compute the SNF of K

$$\begin{aligned} K &= UDV = \begin{bmatrix} x^2-1 & x^3+1 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \ \textit{where} \\ U &= \begin{bmatrix} x^2-1 & x^3+1 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix}, \quad V = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \textit{and} \\ U^{-1} &= \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & x^2-1 & x^3+1 \end{bmatrix}. \end{aligned}$$

The last row of the matrix U^{-1} *is* $U_3 = [1, x^2-1, x^3+1] = [f_1, f_2, f_3]$, *which verifies the result of Theorem 3.2.*

References

[1] W. Adkins and S. Weintraub, *Algebra*, GTM 136, Springer-Verlag, 1992.

[2] V. A. Bovdi and L. A. Kurdachenko, *Modules over some group rings, having d-generator property*, Ricerche mat 71 (2022), 135-145. https://doi.org/10.1007/s11587-021-00581-5.

[3] D. E. Dobbs, *On minimal generating sets of modules over a special principal ideal ring,* Lecture Notes in Pure and Appl. Math, Dekker, New York, 185(1997), 241-250.

[4] D. T. Gué, *Minimum number of generators of the lattice of submodules of a semisimple module,* Journal of Soviet Mathematics, 30 (1985), 1872-1874.

[5] D. Hilbert, *Ueber die Theorie der algebraischen Formen,* Math. Ann., 36 (1890), 473–534.

[6] A. A. Kravchenko, *On the minimum number of generators of the lattice of subspaces of a finite dimensional linear space over a finite field,* Journal of Soviet Mathematics, 27 (1984), No.4.